NANO: Network Access Neutrality Observatory

Mukarram Bin Tariq, Murtaza Motiwala, Nick Feamster
{mtariq,murtaza,feamster}@cc.gatech.edu

ABSTRACT

This paper tackles a technical problem that is of growing interest in light of the ongoing network neutrality debate: We aim to develop a system that can reliably determine whether particular ISP is discriminating against a service using only passive measurements from end-hosts. This problem presents significant challenges because many types of discrimination can often resemble commonplace performance degradations (e.g., resulting from failure or misconfiguration). To distinguish discrimination from degradation, we propose a statistical method to estimate causal effect and develop a system, NANO, based on this method. *NANO* aggregates passive measurements from end-hosts, stratifies the measurements to account for possible confounding factors, and distinguishes when an ISP is discriminating against a particular service or group of clients. Preliminary simulation results demonstrate the promise of *NANO* for both detecting various types of discrimination and absolving an ISP when it is not discriminating.

1. Introduction

Since Ed Whitacre decried content providers ability to "use his pipes [for] free" in November 2005, debate has been raging about the principle of network neutrality—whether an ISP should be able to treat different groups and types of traffic differently (e.g., providing levels of priority, restricting access). There is considerable debate about potential ramifications of net neutrality. In this paper, however, we examine a technical question at the heart of this debate: Can users in access networks collectively detect and quantify discriminatory practices against a particular group of users or services?

Establishing a causal relationship between an ISP's discriminatory behavior and service degradations is challenging since a necessary condition for inferring a valid causal relationship is to show that when all the other *factors* are equal, a service performs poorly when accessed from an ISP compared to another ISP. Unfortunately, many factors can affect the performance of a particular service or application other than ISP discrimination. The service or application may be flawed, or slow at the server end (e.g., due to overload). A service might be poorly located relative to the customers of the ISP. Similarly, it is possible that while the ISP is not meddling with the traffic, the application itself is fundamentally unsuitable for a particular network, e.g., Internet connectivity is not suitable for VoIP applications in many parts of the world. These variables are called *confounding* factors for the causal relationship.

Unfortunately, the nature of many confounding factors makes it difficult to create an environment on the real Internet where all other factors, except for an ISP brand and an application service, would be equal. This makes direct comparison impossible. Instead, *to correctly infer the causal relationship, we must find ways to accurately adjust for the factors other than the discrimination that impact the service performance*.

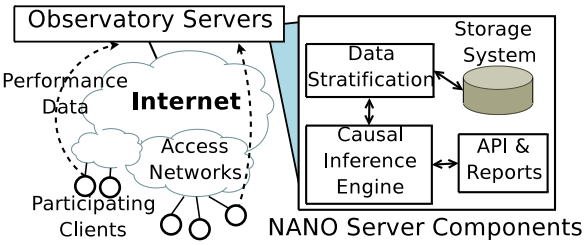


Figure 1: *NANO* Architecture.

Establishing a causal relationship between discrimination and degradation of performance is also difficult because the ISP may discriminate against a service in a variety of ways. For e.g, Comcast and several other ISPs have been interfering with the TCP connections for BitTorrent and other Peer-to-Peer applications [1]. This interference involves injection of TCP reset packets, which are detectable by the clients. Other forms of discrimination might include bandwidth throttling for specific services or treating the traffic in lower QoS class. Unlike, the TCP RST packets, this kind of discrimination does not provide an explicit feedback to the applications, making it difficult to disambiguate server-side problems from ISP's interference.

In this paper, we present the design for Network Access Neutrality Observatory (*NANO*), a system that infers whether an ISP's interference is degrading performance for a particular application or service. *NANO* relies on a set of participating end-system clients that collect and report service performance measurements for a service, as well as values of some of the confounding variables that may be local to the clients. *NANO* uses the collected measurements to adjust for the various confounding factors, including the ones reported by the clients, and infers the extent of causal effect that there is between accessing a service through a particular ISP and service performance. For soundness, *NANO* relies on the theory of causal inference (used extensively in other fields, such as, health, medicine, economics, sociology and epidemiology) and systematically adjusts for confounding variables in the measurements to minimize the risk of false causal assertions. *NANO* can quantify the effect of such discrimination and is also able to infer the criteria that the ISP may use for discrimination.

We present the architecture, design, and algorithm for the *NANO* system. We also present simulation-based results that show that *NANO* can distinguish between server-side problems and ISP discrimination even in subtle cases, and can also detect the discrimination criteria.

This paper is organized as follows. In Section 2 we formu-

late the problem of inferring causal relationship between ISP interference and quality degradation for a service. In Section 3 we present the detailed design for *NANO*, including the confounding variables for the problem, the features that we collect from the clients, and finally the calculation of the causal effect. Section 4 presents simulation-based results. We discuss various limitations and open issues in Section 5, present related work in section 6, and conclude in Section 7.

2. Problem Formulation

In this section, we describe the goals of *NANO* system, and use these to develop a problem statement. In the process, we also describe the various aspects of causal inference theory and how they relate to our problem, and also develop a method for inferring ISP interference in causing performance degradation.

2.1 The Goal of NANO

The goal for *NANO* is to estimate for every ISP and every service that it monitors, if the ISP discriminates against that service. For this, we wish to calculate the causal effect, or a measure of difference in the performance of service when it is accessed through an ISP versus when it is not accessed through that ISP, while adjusting for all the plausible confounding variables.

Concept of Service: A service is defined as the "atomic unit" of discrimination the ISPs can perform. We believe that ISPs have incentive to differentiate against following types of services:

- HTTP traffic identifiable as a particular service, e.g., Web search. Such traffic can be identified by the URL.
- Video traffic, identifiable either from the URL or the application protocol, e.g., RTSP.
- Web traffic for a particular domain, e.g., microsoft.com
- All VoIP traffic or that of a particular VoIP operator.
- Peer-to-Peer traffic identifiable by commonly used port numbers.

Performance: Performance, the outcome variable, has to defined in a way that is appropriate for the service. For example, we use server response time for HTTP requests, loss, and jitter for VoIP traffic, and average throughput for peer-to-peer traffic.

Discrimination: Discrimination against a service is a function of ISP policy. Thus to differentiate it from the physical network that the ISP operates, we use the ISP *brand* as the causal variable. We emphasize *brand* instead of the network as the cause variable to differentiate the inevitable impact on the service performance because of network topology of the ISP, from the intentional and policy based discrimination on the part of the ISP. For example, if a user switches her ISPs because the ISP is discriminating, then with the new ISP, she experiences not just a change in policy but also a different network, with its own characteristics. Thus an objective evaluation of ISP discrimination must adjust for this confounding factor.

2.2 Model for Causal Assertion

There is rich literature in statistics dealing with the subject of causal inference in observational and experimental studies [6, 9]. *NANO* draws heavily on this literature for soundness of methodology. In this section we review relevant concepts of the theory of causal inference and explain how each relates to the problem of inference of ISP's discrimination. We will also develop the notations that we will use later for problem formulation in Section 2.3.

2.2.1 *What is Causality?*

The statement *"X causes Y"* means that we expect a change in value of variable Y, if there is a change in the value of variable X. We refer to X as the treatment variable and Y as the outcome variable that we observe.

In the context of this paper, accessing a particular service through an ISP *brand* is our treatment variable (X), and the observed performance of a service (Y) is our outcome variable. Thus, treatment (X) is a binary variable; $X \in \{0, 1\}$, $X = 1$ when we access the service through the ISP, and $X = 0$ when we do not.

2.2.2 *Association vs. Causal Effect*

Using correlation or association to imply causality is a dangerous fallacy. To avoid this, we have to understand how the two differ and how can they be reconciled.

Lets define *association* as simply the measure of observed effect on the outcome variable in a sample.

$$\alpha = \mathbb{E}(Y|X = 1) - \mathbb{E}(Y|X = 0) \quad (1)$$

Because of confounding variables or certain biases in the dataset, observing association in a sample is not sufficient to assert a causal relationship. To illustrate this and to quantify the causal effect, lets introduce random variables, C_0, and C_1, that correspond to the potential outcome values for $X = 0$ and $X = 1$ respectively, i.e., values of outcome that we will see *if* we set the particular treatment values. For a sample in a dataset, when $X = 1$, we only observe value of C_1 and we do not observe the value of C_0. Similarly, when $X = 0$, C_0 is observed, but C_1 is not. These variables are called *counterfactual variables* because they present the value of outcome under the opposite fact.

We define the *average causal effect* as:

$$\theta = \mathbb{E}(C_1) - \mathbb{E}(C_0) \quad (2)$$

The difference between causal effect and association is that while causal effect is constant for a system irrespective of the dataset, the association depends entirely on the dataset. This means that in general $\alpha \neq \theta$.

Example: Table 1 illustrates the difference between association and causal effect using an example of eight clients (*a–h*). The treatment variable X is binary; 1 if a user uses a particular ISP, and 0 otherwise. For simplicity, the outcome (Y) is also binary, 1 indicating that a client observes high performance and 0 otherwise. The table also presents counterfactual variables C_0, C_1, with '*' indicating the unobserved values, but whose values we know through some kind of an oracle. Note that $Y = C_X$.

	(a) Original Dataset				(b) Active Treatment				(c) Random Treatment	
	X	Y	C_0	C_1	X	Y	C_0	C_1	X	Y
a	0	1	1	1^*	0	1	1	1^*	1	1
b	0	1	1	1^*	0	1	1	1^*	0	1
c	0	1	1	1^*	0	1	1	1^*	1	1
d	0	1	1	1^*	0	1	1^*	1	0	1
e	1	0	0^*	0	0	0	0	0^*	1	0
f	1	0	0^*	0	0	0	0	0^*	0	0
g	1	0	0^*	0	0	0	0	0^*	0	0
h	1	0	0^*	0	1	0	0^*	0	1	0
	$\alpha = -1, \theta = 0$				$\alpha = -3/7, \theta = 0$				$\alpha = 0$	

Table 1: (a) Association (α) is not equal to causal effect (θ). (b) Active Treatment Results in significantly different association. (c) Association estimates causal effect under random treatment assignment.

In Table 1a, the observed values of Y indicate an association of -1, which, if taken as an indication of causal relationship, would imply that the ISP is causing degradation of performance. The values of (unobserved) counterfactuals on the other hand indicate that the performance values for all the customers are agnostic of the choice of ISP; customers *a–d* will have good performance, and customers *e–h* will have poor performance, irrespective of the ISP. Such a situation is easy to conceive; for example, all the users in the first set might be using a better application, e.g., a better Web-browser, which results in better performance, whereas the users in the second set are using a browser that is not well suited for that particular service.

Suppose now that we advise the customers *e–h* to switch to a different ISP, that we believe is not discriminating, and all customers, with exception of customer g, switch. Table 1b shows the values after this active change of treatment. The value of association has become significantly smaller (4/7 - 1 = -3/7), indicating that use of association from the initial dataset to infer causation was wrong. Note that the causal effect remains same, although it is not measurable from the dataset because of the unobservability of the counterfactuals.

2.2.3 *Random Treatment*

Because counterfactuals (C_0, C_1) are not simultaneously observable, we cannot estimate the true causal effect (eq. 2), just from a passive dataset. Fortunately, if we assign the subjects to the treatment in a way that is independent of the outcome, then in certain conditions, association is an unbiased estimator of the causal effect. This holds because when X is independent of C_X, then $\mathbb{E}(C_X) = \mathbb{E}(C_X|X) = \mathbb{E}(Y|X)$; (a formal proof can be found in [9] pp. 254–255). In Table 1c we randomly assign a treatment, 0 or 1, to the clients and we see that α approaches θ.

For association to converge to causal effect with random treatment, all other variables in the system that have a causal association with the outcome variable must remain the same, or change only as a result of the treatment. This requirement can be difficult to satisfy in reality. In the above example, if changing the ISP brand also means that the users must access the content through a radically different network, we cannot use the mere difference of performance seen from the two ISPs as indication of interference: the association may not converge to causal effect under these conditions because the independence condition is not satisfied.

2.2.4 *Adjusting for Confounding Variables without Random Treatment*

Because it is difficult to emulate random treatment on the real Internet (e.g., we cannot ask users to change their ISPs, and even if we could, a change in ISP is accompanied by a change in network), we would like *NANO* to rely mainly on passive measurements. Unfortunately, as we saw in the example in Table 1, passive dataset can be biased and we cannot use association for causal inference.

Fortunately, there is a way to address this problem. If we can find strata within the dataset, such that within each stratum all the samples are very *similar*, then X and C_X are independent, and random-treatment like conditions are created. As a result the association value within the stratum converges to causal effect. The catch is in defining *similar*.

Confounding variables are correlated with both the treatment and the outcome variables. Although there is no automated way of selecting these variables for a particular problem, with sufficient domain knowledge, we can determine the set of such confounding variables with reasonable confidence. Once the confounding variables are known, we can define the similarity based on the closeness in values for the confounding variables. If samples have similar values for confounding factors, and we still observe correlation with the treatment, then we can deduce a causal relationship with confidence.

Let Z denote the set of confounding variables and z a stratum, such that within the stratum the samples are sufficiently similar and the treatment variable is independent of the potential outcome variable, then the association within a stratum is unbiased estimate of causal effect in that stratum [9]:

$$\theta(x; z) = \mathbb{E}(Y|X = x, Z = \mathbb{B}(z)) \quad (3)$$

$$\theta(x) = \sum_z \theta(x; z) \quad (4)$$

$\theta(x; z)$ represents the causal effect within the stratum z, when treatment variable $X = x$. $\mathbb{B}(z)$ represents the values of confounding variables in the stratum z. Finally, the total causal effect for a particular value of X, $\theta(x)$, is simply the sum across all the strata.

2.3 Formal Problem Statement

We wish to calculate the causal effect θ_{ij} that estimates how much the of a service j, denoted by Y_j changes, when it is accessed through ISP i, versus when it is not accessed through ISP i, while adjusting for all the plausible confounding variables Z. Based on Eq. 3 and Eq. 4, overall causal effect, θ_{ij}, and causal effect within each stratum, $\theta_{ij}^{(z)}$ is:

$$\theta_{ij} = \sum_z \theta_{ij}^{(z)} \quad (5)$$

$$\theta_{ij}^{(z)} = \theta_{ij}(1; z) - \theta_{ij}(0; z) \quad (6)$$

$$\theta_{ij}(x; z) = \mathbb{E}(Y_j|X_i = x, Z = \mathbb{B}(z)) \quad (7)$$

NANO should raise an alarm when it confidently infers a sufficiently negative causal effect for a particular service or a particular stratum of a service. The following section details how *NANO* addresses the challenges in collecting the data and computing this causal effect.

3. NANO Design

The key challenges that *NANO* addresses are: (1) presenting a plausible set of confounding variables for the prob-

lem of asserting ISP interference that results in performance degradation, (2) devising mechanisms that can passively collect necessary data to allow adjusting for the confounding variables while estimating the causal effect, and finally (3) quantifying the causal effect and inferring the criteria for discrimination that an ISP may be using.

3.1 Confounding Variables

Accounting for all plausible confounding variables is critical for passive causal inference, but unfortunately, there is no automated way of discovering what is a sufficient set of confounding variables for a given experiment; instead we must rely on domain-specific knowledge. The following list of confounding variables are necessary for inferring causal effect for neutrality; we divide these variables in three categories.

Client-based: The particular application that a client uses for accessing a service might affect the performance. For example, in the case of HTTP services, certain websites may be optimized for a particular Web-browser, and perform poorly for others. Similarly, certain Web-browsers may be inherently different, e.g., at the time of this writing, Opera, Firefox and Internet Explorer use different number of simultaneous TCP connections, and only Opera uses HTTP pipelining by default. Similarly, the operating system and the configuration of the client's computer can have an impact on performance.

Network-based: Various properties of the Internet path, like location from the ISP to the service, can cause performance degradation for a service; such degradation is not discrimination. Similarly, there can be situations where a segment on path to a particular service provider is not sufficiently provisioned and results in a degradation. If we wish to not treat the effects of such a factor as discrimination, we should adjust for the path properties.

Time-based: Service performance varies widely with time-of-the-day due to changes in utilization. We can have two datasets where all the confounding factors are similar but just because the datasets are collected at different times of the day, we will see difference in performance that can be misinterpreted for discrimination.

NANO uses basic sanity checks to verify that the confounders that we consider are sufficient (Section 3.3.1). While such sanity checks can reveal insufficiency of the variables, the burden of finding a sufficient set of variables is still on domain knowledge.

3.2 Data Collection

Here we describe the criteria and mechanism of collection, attributes that *NANO* collects and the storage of the data.

1. Criteria: *NANO* collects statistics that would help infer the following: name of the ISP that is monitored, the value for service performance, and the values for each of the confounding variables for each sample.

Because an ISP can easily treat any explicit probing traffic differently, use of explicit probes can introduce biases. For this reason, *NANO* relies on inferring performance using passive means to the extent possible.

2. Mechanism: The primary source for data for *NANO* is a client-side agent installed on computers of voluntarily participating clients(*NANO*-Agent). This agent continuously monitors and reports the data to the *NANO* servers. We are developing two versions of this agent: first is a Web-browser plug-in that can monitor Web-related activities, and second is a self contained binary that can access more fine-grained information from the client machines.

3. Dataset Attributes: *NANO*-Agent collects three sets of attributes. First it collects attributes that help identify the client setup, including the operating system, basic system configuration and resource utilization on the client machine.

Second, the *NANO*-Agent monitors and logs the information about the ongoing traffic from the client machine for the services that we request to monitor. In particular, the standalone binary version logs the RTT measurements to various destinations for small and large (MTU) sized packets. *NANO*-Agent also collects unsampled netflow style statistics for the ongoing flows, and also maintains the applications associated with each flow. Finally, *NANO*-Agent tags this information with a service identifier that it infers by inspecting the packet payloads (e.g., by looking for regular-expression 'google.com/search?q=' in the HTTP request message to identify search service), or just by looking at the protocol and port numbers where possible. The Web browser plug-in version of the *NANO*-Agent only monitors the Web traffic.

Finally, *NANO*-Agents perform active measurements to a corpus of diverse benchmark sites (PlanetLab nodes) to establish the topological location of the clients and their ISPs. These measurements include periodic short and long transfers with the benchmark sites. These measurements are similar in spirit to ones used by many Internet coordinate systems [2]. *NANO* uses this information to establish the topological properties of the ISP and stratify ISPs with similar topological location to adjust path properties factor. All the data is time-stamped to allow adjustment for time-of-the-day factor and aggregated at a central storage system. *NANO*-Agent is similar

3.3 Causal Effect Estimation

Causal Effect estimation involves three steps. First we stratify the data, then we estimate the extent of causal impact of possible ISP interference within each stratum and across the board. Finally we try to identify the criteria that the ISP is using for discrimination.

3.3.1 *Creating the Strata*

We need strata such that the data samples within each stratum are similar. For this, *NANO* creates partitions along the dimensions of each of the confounding variables, such that the value of the confounding variable within the strata is (almost) constant. For example, the variable representing the client browser, all the clients using a particular version and make of the browser are in one strata. Similarly, we create one hour strata along the time-of-the-day variable. We also stratify the ISPs based on their connectivity to the benchmark sites, with particular /24 subnets across ISPs that seem to have similar topological reference and connectivity belonging in the same stratum; for this again we use small

bins as boundaries of strata along the dimensions of average TCP SYN-SYN/ACK RTT, and average upload and download speeds for short and long lived transfers. Similarly, we use the application identifiers and client-setup parameters as additional dimensions for stratification; all the data-points in a stratum have similar values for the client setup and application.

The strata partition the space such that each partition is a high-dimensional hyper-rectangle; these rectangles are packed tightly to cover the entire dataset space; the samples falling within a particular rectangle are similar along all features except for the treatment variable (the choice of the ISP) and the outcome (the performance for a particular service).

As a sanity check of correct stratification and whether we are capturing all the confounding variables, we perform random test to verify that the distribution of performance for clients in a particular stratum are similar; we use two-sample Kolmogov-Smirnov test for this purpose.

3.3.2 *Estimating the Extent of Causal Impact*

Estimating the causal effect follows directly from Eq. 6 and Eq. 7. For each stratum z, *NANO* uses the boundary conditions for the stratum as $\mathbb{B}(z)$, and calculates $\theta_{ij}(1;z)$ for each service j for each ISP i, in a straightforward manner. Calculating $\theta_{ij}(0;z)$, unfortunately, is tricky. It raises the question: What does it means to not use ISP i? Does this mean using another ISP, because the clients need to access the Internet through some ISP k to get any kind of measurements. But, if ISP k is also discriminating against service j, then θ_{kj} will not have the (neutral) counterfactual value. We address this problem by instead taking $\theta_{ij}(0;z)$ as average effect expected when not using ISP i, calculated as:[1] $\sum_{k\neq i}\theta_{kj}(1;z)/(n_z-1)$; here n_z is the number of ISPs for which we have clients in stratum z. With this we can calculate the causal effect within each stratum, $\theta_{ij}^{(z)}$, as well as the overall causal effect, θ_{ij}. Because the units of causal effect are same as the service performance, we can use simple thresholds to detect extra-ordinary discrimination.

3.3.3 *Inferring the Discrimination Criteria*

NANO can infer the discrimination criteria that an ISP uses by using simple decision-tree based classification methods. For each stratum and service where *NANO* detects discrimination, we assign a negative label, and for each stratum and service where we do not detect negative discrimination, we assign a positive label. We use the values of the confounding variables and the service identifier as the feature set and use the discrimination label as the target variable, and use a decision-tree algorithm to train the classifier. The rules that the decision-tree generates indicate the discrimination criteria that the ISP uses, because the rules indicate the boundaries of maximum information distance between discrimination and lack of it.

4. Evaluation

We present simulation based results for detecting situations where an ISP might discriminate against a particular service. Our simulation setup comprises two ISPs, ISP_A, and ISP_B that provide connectivity for their respective clients to two websites WS_1 and WS_2. The clients comprise of two processes, each repeated requesting a random resource from one of the two websites. We collect traces that identify the client, its ISP, the server that it accessed, the RTT to the servers, and the response time for each request.

We perform three experiments of increasing complexity. In the first experiment, we show that we can identify a server-side problem from network discrimination. In the second experiment, we simulate the case of a simple discrimination where an ISP degrades the performance for one of the two sites for all of its clients. In the third case one ISP has clients of two different priority classes, and it selectively restricts the access to one of websites for its low priority clients. In each of these cases we assume that ISP topology is not a confounding factor for simplicity; this confounding factor, as we discussed earlier, can be adjusted by calibrating against the benchmark sites in the *NANO* system.

WS_2 is slow for the clients: This experiment simulates a condition where a website may be slow for all the clients irrespective of the ISP, because the site is either poorly located or poorly designed. We wish to distinguish this case from ISP discrimination. The top half in Figure 2a shows the response time for the two ISPs and the two websites. The graph clearly shows that WS_2 is slow, but this analysis alone does not absolve the ISPs. In the lower part we stratify the same measurements, and show that WS_2 is slow irrespective of the ISP, thus it is likely not a case of discrimination. This fact is also reflected in the measured causal effect $\theta_{B,2}=-1.1ms$, which is small compared to average performance of 13ms from WS_2 for all clients.

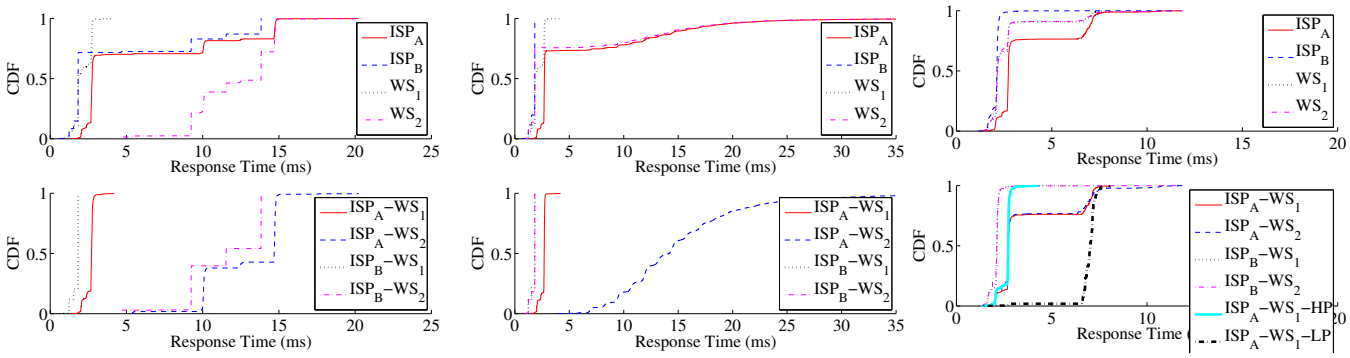
ISP_A discriminates against WS_2: In this experiment ISP_A throttles the bandwidth for WS_2 for all its clients. Top subplot in Figure 2b shows the performance for each ISP and website. ISP_A and WS_2 have certain performance problems, but the cause is not clear. The bottom subplot shows the results after stratification; *NANO* determines $\theta_{A,2}=-13.5ms$, which is nearly 10 times the average latency from WS_2 to other clients; we can blame ISP_A here.

ISP_A selectively discriminates against WS_2: In this experiment ISP_A has two priority classes for its customers. The high priority clients are unrestricted and also have a higher QoS priority. The low priority clients have unrestricted access to WS_1 within their priority class, but the access to WS_2 is further throttled. In this case *NANO* identifies that the clients of ISP_A to belong to two different classes and places them in different strata. Figure 2 shows that the full extent of the effect of discrimination does not come out until full stratification, whereupon we find $\theta_{A,2}^{(HP)}=-6.9ms$, which is nearly 3 times the average performance of WS_2 to clients of ISP_B.

5. Discussion

We discuss several open issues. First, should we be using a generic approach like in *NANO*, or look for specific tell-tale signs, such as, TCP reset packets, traffic shaping (e.g., Comcast provides a bandwidth boost at the start of connections)? We argue that while it might be easier to detect such tell-tale signs, doing so results in a cat-and-mouse game, where

[1] We also consider other metrics, e.g., minimum causal effect within the strata, and the causal effect on *equivalent* services. These metrics are not described because of lack of space.



(a) WS_2 is slow irrespective of the ISP (b) ISP_A discriminates WS_2 (c) ISP_A selectively discriminates WS_1

Figure 2: Simulation setup and results on causal inference.

we will not be able to detect changes without someone first making an insightful observation that can lead to further investigation and automation of detection.

Second, can *NANO* differentiate network faults from discrimination? We believe that the network faults are transient in nature, whereas discrimination is a persistent phenomena. We can adjust the thresholding mechanism in *NANO* to differentiate transient problems from the persistent ones.

Because some of the measurements that *NANO*-Agent collects can lead to invasion of user privacy, *NANO* stores the data in a stratified form and does not maintain any client-identifiable data (e.g., client IP addresses or search queries). Further, *NANO* delegates some of the stratification tasks to the agents on the clients, so that most of the user-identifiable data does not leave the client in the first place. This mitigates some of the privacy concerns.

To provide users an incentive to install *NANO* clients, we plan to provide the users with a feedback on their and other ISP's performance, as well as other network diagnostics aid that the collected data can facilitate. Addressing privacy issues and recruitment sufficient number of clients that can provide reasonable amount of data for causal inference remains an open problem.

6. Related Work

This section surveys previous projects that have attempted to characterize performance issues or various types of discrimination in ISPs. Glasnost [1] detects TCP reset poisoning for connections of Peer-to-Peer applications. Tripwire [7] uses a fingerprinting-based technique to detect modification of in-flight packets, such as for insertion of advertisements. This is an important class of neutrality violation, but we focus on violations that result in discrimination and performance degradation.

NetDiff[5] detects performance differences among Backbone ISPs. NetDiff uses the geolocation and spread as a normalizing factor for fair comparison between ISPs, and in a sense adjusts for a confounding factor in the assertion that one ISP is better than another. *NANO*'s agenda is detecting per-service discrimination which introduces additional confounding factors. Yang et al. [10] propose a way of preventing ISPs from discriminating against packets altogether, but they require changes to user traffic (e.g encryption) unlike *NANO* which only detects discrimination based on passive measurements. *NANO* can also draw on previous work on characterizing ISP networks [4] and monitoring ISP SLA[8] to adjust for ISP topology differences. Finally, we hope that we can use SatelliteLab [3] nodes to directly emulate random-treatment on the Internet; unfortunately, at this time, the *satellite* nodes in the SatelliteLab system only support relaying the traffic that the *planet* nodes generate, which introduces an additional confounding factor.

7. Conclusion

We presented Network Access Neutrality Observatory (*NANO*), a system for inferring whether an ISP is discriminating against a particular service. Existing systems for monitoring network neutrality check for known tell-tale signs of discrimination; *NANO* is the first system that relies on general statistical performance comparisons to detect discrimination. In this paper, we have examined only basic criteria for discrimination in a simulation environment; in future work, we will evaluate *NANO*'s effectiveness in the wide area, for a wider range of possible discrimination activities, and in adversarial settings where the ISPs may attempt to evade detection.

REFERENCES

[1] Glasnost: Bringing Transparency to the Internet. http://broadband.mpi-sws.mpg.de/transparency/.

[2] F. Dabek, R. Cox, F. Kaashoek, and R. Morris. Vivaldi: A decentralized network coordinate system. In *Proc. ACM SIGCOMM*, Portland, OR, Aug. 2004.

[3] M. Dischinger, A. Haeberlen, I. Beschastnikh, K. Gummadi, and S. Saroiu. SatelliteLab: Adding Heterogeneity to Planetary-Scale Testbeds. In *Proc. ACM SIGCOMM*, Seattle, WA, Aug. 2008. (To appear).

[4] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. E. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An information plane for distributed services. In *Proc. 7th USENIX OSDI*, Seattle, WA, Nov. 2006.

[5] R. Mahajan, M. Zhang, L. Poole, and V. Pai. Uncovering Performance Differences among Backbone ISPs with Netdiff. In *Proc. 5th USENIX NSDI*, San Francisco, CA, Apr. 2008.

[6] J. Pearl. *Causality: Models, Reasoning, and Inference.* Cambridge University Press, 2000.

[7] C. Reis, S. D. Gribble, T. Kohno, and N. C. Weaver. Detecting in-flight page changes with web tripwires. In *Proc. 5th USENIX NSDI*, San Francisco, CA, Apr. 2008.

[8] J. Sommers, P. Barford, N. Duffield, and A. Ron. Efficient Network-wide SLA Compliance Monitoring. In *Proc. ACM SIGCOMM*, Kyoto, Japan, Aug. 2007.

[9] L. Wasserman. *All of Statistics: A Concise Course in Statistical Inference.* Springer, 2003.

[10] X. Yang, G. Tsudik, and X. Liu. A technical approach to network neutrality. In *Proc. 5th ACM Workshop on Hot Topics in Networks (Hotnets-V)*, Irvine, CA, Nov. 2006.